PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-285156
(43)Date of publication of application : 23.10.1998

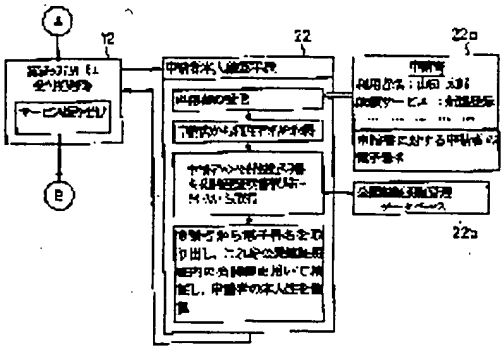
(51)Int.Cl. H04L 9/32
H04L 9/08

(21)Application number : 09-092436
(22)Date of filing : 10.04.1997

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
N T T SOFTWARE KK
(72)Inventor : HASHIMOTO SHOICHI
MURATA YUICHI
NAKAHARA SHINICHI

(54) USER INFORMATION MANAGEMENT DEVICE IN AUTHENTICATION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To automatically recognize and update only self-user information and to reduce the trouble of the management of user information, which an authentication system executes, by permitting the user to send an application to the authentication system by adding an electronic signature.
SOLUTION: When the user applies service request to an authentication system service reception processing part 12, an applicant original recognition means 22 is called and the application 22a is received by using an electronic mail or the like. An applicant name is obtained from the application 22a and an open key certificate is read from an open key management data base. The electronic signature is fetched from the application 22a and it is verified by the open key in the open key certificate so as to recognize the rightness of the user. The open key certificate of the applicant can be obtained from an open key certificate management data base 22b and the electronic signature of the application 22a can be verified by an open key certificate reference function and an electronic signature verification function, which are generally prepared in the verification system.



LEGAL STATUS

[Date of request for examination] 01.02.2001
[Date of sending the examiner's decision of rejection] 13.04.2004

CLAIMS

[Claim(s)]
[Claim 1] It is user information management equipment in the authentication system using the public key cryptosystem which manages the public key certification certificate proving being the owner of the public key specified with the user information which is the information concerned which has and mainly starts. The user information management table on which said user information is managed by the user name concerned, the time of there being an application of a printing demand on this user information management table -- the user name of this application -- an applicant -- the applicant who checks whether you are a principal -- a principal -- with a check means this applicant -- a principal check means -- said user name -- an applicant -- the user information management equipment in the authentication system characterized by having a printing means to carry the user information concerned for every user on said user information management table when it is checked that he is a principal.
[Claim 2] It is user information management equipment in the authentication system using the public key cryptosystem which manages the public key certification certificate proving being the owner of the public key specified with the user information which is the information concerned which has and mainly starts. Said user information The user information management table concerned which has and is managed by the main user names, the user name for which it applied on the occasion of utilization of this user information management table -- an applicant -- the applicant who checks whether you are a principal -- a principal -- with a check means It is checked that he is a principal. this applicant -- a principal check means -- said user name -- an applicant -- User information management equipment in the authentication system characterized by having a deletion means to delete the user information concerned from a user information management table when said application is deletion of the user information concerned from a user information management table which has and mainly starts.
[Claim 3] It is user information management equipment in the authentication system using the public key cryptosystem which manages the public key certification certificate proving being the owner of the public key specified with the user information which is the information concerned which has and mainly starts. Said user information The user information management table concerned which has and is managed by the main user names, the user name for which it applied on the occasion of utilization of this user information management table -- an applicant -- the applicant who checks whether you are a principal -- a principal -- with a check means It is checked that he is a principal. this applicant -- a principal check means -- said user name -- an applicant -- User information management equipment in the authentication system characterized by having the user information management table retrieval means which searches the information management table concerned and reads applicable user information when said application is read-out of the user information from a user information management table.
[Claim 4] It is user information management equipment in the authentication system using the public key cryptosystem which manages the public key certification certificate proving being the

owner of the public key specified with the user information which is the information concerned which has and mainly starts. Said user information The user information management table concerned which has and is managed by the main user names, the user name for which it applied on the occasion of utilization of this user information management table -- an applicant -- the applicant who checks whether you are a principal -- a principal -- with a check means It is checked that he is a principal. this applicant -- a principal check means -- said user name -- an applicant -- User information management equipment in the authentication system characterized by having a renewal means of a user information management table to update to the user information to which it applied for the applicable user information on the information management table concerned when said application was renewal of the user information carried by the user information management table.

[Translation done.]

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the user information management equipment in the authentication system proving the justification of the public key used by the public key cryptosystem.
[0002]
[Description of the Prior Art] In case an electronic data exchange (EDI:Electronic Data Interchange) and electronic commerce (EC:Electronic Commerce) are realized on a computer network, threats, such as tapping / spoofing / alteration / transmitting denial, are assumed. Therefore, in order to defend a system from these threats, generally cryptocommunication and a digital signature communication link are used. This cipher system is announced by reference "Diffie, W.and Helman, M.:New Directions in Cryptography, IEEE Trans.Inf.Theory, IT-22, 6 pp.644-654, and 1976", and serves as a place widely known in the world.
[0003] In such a public key cryptosystem, a communication link is performed using two kinds of keys, the public key generally exhibited widely and the private key which he can know. The independent organization proving being the just owner of a public key only by a public key being well-known, here, since the threat called "spoofing" which is well-known pretending to be others can be considered is required, and it is called a certificate authority (CA:Certification Authority).
[0004] In case the authentication system containing this certificate authority realizes electronic commerce which transmits and processes information on a computer network on the electronic data exchange which carries out the electronic automatic exchange of the dealings between the enterprises in business connections, or a computer network, and performs business, such as electronic banking, it is a system which is related with the public key cryptosystem used for the secrecy nature of transmit data, or the object of alteration prevention, and publishes / manages that public key certification certificate. That is, it can be said that it is the Japanese actual world, and an authentication system is the world of digital communication and is a system with the function to publish the public key certification certificate proving the owner of a public key as a government office publishes the certificate of the seal impression proving the owner of a legal seal.
[0005] Generally the following four are known as a function of an authentication system.
(1) Public key add function -- A public key certification certificate is created, registered / published to the public key for which the user applied.
(2) Certification certificate reference function -- Reference of the public key certification certificate managed by the authentication system is enabled from a user.
(3) Public key nullification function -- A public key certification certificate is cancelled and it carries on a nullification list.
(4) Nullification list reference function -- Reference of the list of the cancelled public key certification certificates is enabled from a user.

[0006] These functions can be built using the general means already offered by a computer system and cryptographic algorithm, and it is recognized as it being already the general approach also about fundamental configuration methods, such as performing the request which used the application at the time of an application, performing a digital signature communication link between an authentication system and a user, and managing a public key certification certificate and a nullification list in a directory or a database.
[0007] Now, an authentication system will extract required information from the application which a user presents, and will create a public key certification certificate. However, the application presented by this user is usually asked for the publication of the information which is information required for management of an authentication system for an authentication system to take contact with a user, the account information for performing accounting, etc. besides information required for creation of a public key certification certificate. Therefore, user information which is a user individual's information which is not put on these public key certification certificates is usually made another management with the public key certification certificate in the interior of an authentication system so that it may not leak outside. Moreover, in case the management person of an authentication system referred to the individual humanity news of the user concerned using these user information, the management person concerned was made to search the inside of a system separately by using a user name etc. as a search key.

[0008]
[Problem(s) to be Solved by the Invention] However, apart from the public key certification certificate opened to a world, since the user information which is not put on a public key certification certificate in the information for which a user usually applies to an authentication system is closed and managed inside the authentication system, it is difficult for a user to perform actuation of his check and updating to user information, without through the management person of an authentication system.
[0009] For example, he expects that a user performs advice to the user concerned about the advice approach of communication for a user from an authentication system using an electronic mail, and when are seen about the case where it has applied for that as individual humanity news and a user's system stops for a certain reason, a user has to apply for changing into advice by mail. In such a case, a user cannot update by carrying out direct access to the user information managed by these authentication systems, and checking the content of printing. Therefore, a user will ask an authentication system, and will have an operator check the actual condition, the time and effort of applying for a modification request after that will be taken, and a load will be applied to the management to the user information on an authentication system.
[0010] Moreover, when the nullification application of the public key certification certificate which cancels the public key certification certificate concerned is made by the user and a user's public key certification certificate is lost in an authentication system, for example by him, the need of also managing the user's individual humanity news will be lost, but since user information is another managed, it serves as [that the user's user information is left behind with as, and] a public key certification certificate. Therefore, the problem that user information is not managed certainly may produce that possibility that futility will arise is in the storage region which manages user information etc.
[0011] This invention was made in view of the above-mentioned technical problem, and required user information is received in management of an authentication system. He is enabled for a user to do direct access, and to check and update only to his information. Moreover, an authentication system It relates with management of a public key certification certificate, registration and deletion of user information are performed, and it aims at offering the user information management equipment in the authentication system which makes it possible to manage user information certainly.
[0012]

[Means for Solving the Problem] In order to attain the object mentioned above, among this inventions invention according to claim 1 It is user information management equipment in the authentication system using the public key cryptosystem which manages the public key certification certificate proving being the owner of the public key specified with the user information which is the information concerned which has and mainly starts. The user information management table on which said user information is managed by the user name concerned, the time of there being an application of a printing demand on this user information management table -- the user name of this application -- an applicant -- the applicant who checks whether you are a principal -- a principal -- with a check means this applicant -- a principal check means -- said user name -- an applicant -- when it is checked that he is a principal, let it be a summary to have a printing means to carry the user information concerned for every user on said user information management table.

[0013] In this invention according to claim 1, the individual humanity news of the user who does not put on a public key certification certificate When a user name is used as a key like a public key certification certificate, an authentication system manages and a printing demand on a user information management table is from a user to a principal's user information After checking automatically, the actuation to user information is permitted and applications of printing, such as new registration of the public key certification certificate from a user, are received. the electronic signature attached to the application -- verifying -- the principal, an applicant, -- as a part of these processings A printing means is enabled to register user information if needed.

[0014] It is user information management equipment in the authentication system using the public key cryptosystem which manages the public key certification certificate which proves that invention according to claim 2 is the owner of the public key specified among this inventions with the user information which is the information concerned which has and mainly starts. Said user information The user information management table concerned which has and is managed by the main user names, the user name for which it applied on the occasion of utilization of this user information management table -- an applicant -- the applicant who checks whether you are a principal -- a principal -- with a check means this applicant -- a principal check means -- said user name -- an applicant -- it is checked that he is a principal, and when said application is deletion of the user information concerned from a user information management table which has and mainly starts, let it be a summary to have a deletion means to delete the user information concerned from a user information management table.

[0015] In this invention according to claim 2, the individual humanity news of the user who does not put on a public key certification certificate When a user name is used as a key like a public key certification certificate, an authentication system manages and there is a deletion demand from a user information management table from a user to a principal's user information the electronic signature attached to the application -- verifying -- the principal, an applicant, -- after checking automatically, the actuation to user information is permitted and a deletion means is enabled to delete user information as a part of these processings.

[0016] It is user information management equipment in the authentication system using the public key cryptosystem which manages the public key certification certificate which proves that invention according to claim 3 is the owner of the public key specified among this inventions with the user information which is the information concerned which has and mainly starts. Said user information The user information management table concerned which has and is managed by the main user names, the user name for which it applied on the occasion of utilization of this user information management table -- an applicant -- the applicant who checks whether you are a principal -- a principal -- with a check means It is checked that he is a principal. this applicant -- a principal check means --,said user name -- an applicant -- When said application is read-out of the user information from a user information management table, let it be a summary to have the user information management table retrieval means which searches the information management table concerned and reads applicable user information.

[0017] In this invention according to claim 3, the individual humanity news of the user who does not put on a public key certification certificate When a user name is used as a key like a public key certification certificate, an authentication system manages and there is a read-out demand of a user information management table to a principal's user information from a user to a principal's user information, the electronic signature attached to the application is verified. the principal, an applicant, -- after checking automatically, the actuation to user information is permitted and a user information management table retrieval means makes it possible to search a user information management table and to read user information as a part of these processings.

[0018] It is user information management equipment in the authentication system using the public key cryptosystem which manages the public key certification certificate which proves that invention according to claim 4 is the owner of the public key specified among this inventions with the user information which is the information concerned which has and mainly starts. Said user information The user information management table concerned which has and is managed by the main user names, the user name for which it applied on the occasion of utilization of this user information management table -- an applicant -- the applicant who checks whether you are a principal -- a principal -- with a check means It is checked that he is a principal. this applicant -- a principal check means -- said user name -- an applicant -- When said application is renewal of the user information carried by the user information management table, let it be a summary to have a renewal means of a user information management table to update to the user information to which it applied for the applicable user information on the information management table concerned.

[0019] In this invention according to claim 4, the individual humanity news of the user who does not put on a public key certification certificate When a user name is used as a key like a public key certification certificate, an authentication system manages and there is an updating demand of modification of user information, an addition, correction, etc. from a user to a principal's user information the electronic signature attached to the application -- verifying -- the principal, an applicant, -- after checking automatically, the actuation to user information is permitted and the renewal means of a user information management table is enabled to update user information as a part of these processings.

[0020]

[Embodiment of the Invention] Hereafter, the gestalt of operation of this invention is explained using a drawing. Drawing 1 is the block diagram showing the configuration of the authentication system concerning the gestalt of 1 operation of this invention. An authentication system 1 is constituted in drawing 1 by the activation means 20 established corresponding to the processing section 10 and this processing section 10. The processing section 10 is constituted by the initial generation processing section 11 of a system, the authentication system service reception processing section 12, the user new registration processing section 13, the public key certification certificate nullification processing section 14, the user information acknowledge request processing section 15, and the renewal demand processing section 16 of user information.

[0021] moreover Corresponding to the initial generation processing section 11 of a system, it corresponds to the user information management table creation means 21 and the authentication system service reception processing section 12. Corresponding to the principal check means 22 and the user new registration processing section 13, it corresponds to the printing means 23 to a user information management table, and the public key certification certificate nullification processing section 14. an applicant -- Corresponding to the deletion means 24 from a user information management table, and the user information acknowledge request processing section 15, the renewal means 26 of a user information management table is established corresponding to the user information management table retrieval means 25 and the renewal demand processing section 16 of user information.

[0022] Hereafter, an operation of the activation means in each processing section is explained according to procedure. First, user information management table 21a which uses a user name as shown in drawing 2 as a key in the initial generation processing section 11 of a system at step S1 using the user information management table creation means 21 is prepared.
[0023] continuing step S2 -- the authentication system service reception processing section 12 -- setting -- an applicant -- a principal -- verifying the electronic signature given by application 22a whether there is any falsehood in the applicant name indicated by application 22a which received using the check means 22 -- a principal -- a sex is checked.
[0024] Next, when the service which the applicant requested to the authentication system is new registration service, it progresses to step S3, a user name and user information are read from application 22a in the user new registration processing section 13 using the printing means 23 to user information management table 21a, and this is carried to user information management table 21a.
[0025] moreover, when the service which the applicant requested to the authentication system is public key certification certificate nullification service Progress to step S4 and the deletion means 24 from user information management table 21a is used in the public key certification certificate nullification processing section 14. After an applicant's public key certification certificate confirms not remaining in public key certification certificate management database 24a shown in drawing 5 , the user's item (a user name, user information) in user information management table 21a is deleted.
[0026] Moreover, when the service which the applicant requested to the authentication system is check service of user information, it progresses to step S5, the corresponding user information is acquired in the user information acknowledge request processing section 15 using the retrieval means 25 of user information management table 21a, and the information is sent to an applicant.
[0027] Furthermore, when the service which the applicant requested to the authentication system is updating service of user information, it progresses to step S6, and in the renewal demand processing section 16 of user information, using the updating means 26 of user information management table 21a, the user information of the applicable user in user information management table 21a is transposed to the user information to which it applied, and is updated.
[0028] Next, the processing in this operation gestalt is explained to a detail for every processing section. First, with reference to drawing 2 , the initial generation processing of a system in the initial generation processing section 11 of a system is explained. Various kinds of initialization processings are performed in the initial generation processing section 11 of a system of an authentication system. As a part of the processing, the user information management table creation means 21 is called first. With the user information management table creation means 21, a table storage region is secured and user information management table 21a which has the description column of a user name and user information as shown in drawing 2 in this secured field is created. Here, a table storage region may exist anywhere on memory or secondary storage media, such as a magnetic disk, and the partitioning is realized by the function which the general computer system offers.
[0029] Next, with reference to drawing 3 , the authentication system service reception processing in the authentication system service reception processing section 12 is explained. If the application of a service request is made from a user to an authentication system, authentication system service reception processing will be carried out in an authentication system. as a part of the processing -- an applicant -- a principal -- the check means 22 is called. an applicant -- with the principal check means 22, application 22a is received, an applicant name is acquired from application 22a, and an applicant's public key certification certificate is read from a public key management database. Next, the electronic signature given to application 22a is taken out, this is verified using the public key contained in a public key

certification certificate, and this human nature of an applicant, i.e., the justification as a user, is checked.

[0030] In addition, reception of application 22a is realizable using the approach which the computer system generally offers, for example, an electronic mail etc. Moreover, verification of acquisition of the public key certification certificate of the applicant from a public key certification certificate management database and the electronic signature of application 22a is realizable by using the public key certification certificate reference function and electronic signature verification function which are generally prepared by the authentication system.

[0031] Next, with reference to drawing 4 , the user new registration processing in the user new registration processing section 13 is explained. In new registration service, by service distribution processing [in / in the service for a request indicated by application 22a received from the user / the authentication system service reception processing section 12], processing moves to the user new registration processing section 13, and the printing means 23 to user information management table 21a is called there. With the printing means 23 to user information management table 21a, a user name and user information are read from application 22a, to user information management table 21a, a user name and user information are matched and this is carried. About the printing approach at this time, it is realizable with the write-in function of the information which a general computer system offers according to the location where the table storage region is secured.

[0032] Next, with reference to drawing 5 , the public key certification certificate nullification processing in the public key certification certificate nullification processing section 14 is explained. In public key certification certificate nullification service, processing moves to the public key certification certificate nullification processing section 14 by service distribution processing [in / in the service for a request indicated by application 22a received from the user / the authentication system service reception processing section 12]. In the public key certification certificate nullification processing section 14, the public key certification certificate for [for which the user applied] nullification is registered into a nullification list, and processing in which the public key certification certificate is deleted from public key certification certificate management database 24a which an authentication system manages is performed. At this time, the deletion means 24 from user information management table 21a is called as a part of this processing.

[0033] With the deletion means 24 from user information management table 21a, first, a user name is read from application 22a, and the user's public key certification certificate checks not remaining any longer in public key certification certificate management database 24a which an authentication system manages. Since the need that an authentication system manages the user's user information is lost when the user's public key certification certificate does not remain in an authentication system here, the user's item (a user name and user information) is deleted from user information management table 21a. This enables it to use the management domain of user information without futility.

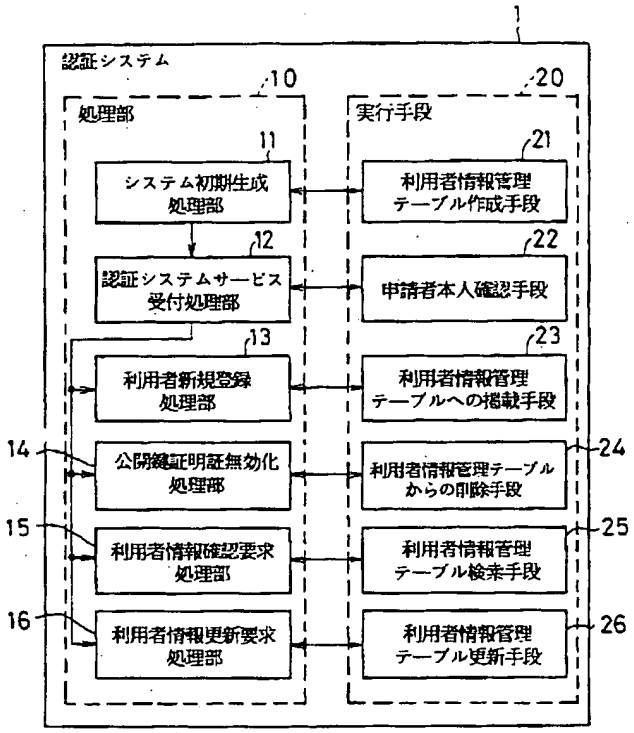
[0034] In addition, retrieval of public key certification certificate database 22b is easily realizable with the function which the usual authentication system holds.

[0035] Next, with reference to drawing 6 , the user information acknowledge request processing in the user information acknowledge request processing section 15 is explained. In user information check service, processing moves to the user information acknowledge request processing section 15 by service distribution processing [in / in the service for a request indicated by application 22a received from the user / the authentication system service reception processing section 12]. the user information acknowledge request processing section 15 -- an applicant -- an acknowledge request is received only to a principal's user information. here -- an applicant -- a principal -- the check means 22 -- setting -- a principal -- the applicant to whom check processing was given -- check processing is received only within only a principal's user information.

[0036] then, the user information management table retrieval means 25 -- calling -- a principal -- the user name indicated in the application with which the check ended is acquired, and user information management table 21a is searched with this user name. And an applicant enables it to check his user information by reading the user information applicable to the searched user name, and sending this to an applicant.
[0037] In addition, retrieval of user information is easily realizable by using the information retrieval technique currently offered in the general computer system.
[0038] Next, with reference to drawing 7 , the renewal demand processing of user information in the renewal demand processing section 16 of user information is explained. In the renewal service of user information, processing moves to the renewal demand processing section 16 of user information by service distribution processing [in / in the service for a request indicated by application 22a received from the user / the authentication system service reception processing section 12]. the renewal demand processing section 16 of user information -- an applicant -- an updating demand is received only to a principal's user information. here -- an applicant -- a principal -- the check means 22 -- setting -- a principal -- the applicant to whom check processing was given -- an update process is received only within only a principal's user information.
[0039] Then, the renewal means 26 of a user information management table is called, and a user name and the update information of user information are first acquired from application 22a. Next, in user information management table 21a, a user name is searched, and the column of the user information of the corresponding user is transposed to update information, and is updated.
[0040] In addition, the renewal of the user information column in user information management table 21a is easily realizable by using the write-in function of the information currently offered in the general computer system.
[0041] By the above processing, the actuation request to an applicant's user information is completed. As mentioned above, according to this operation gestalt, only by a user's attaching electronic signature to application 22a, and sending to an authentication system, only within their user information, the check and processing of updating can be performed automatically, and the time and effort of the management of user information which an authentication system performs by this is mitigated. Moreover, it becomes possible by associating new registration processing of a public key certification certificate, nullification processing, and registration of user information and processing of deletion to ensure management of user information.
[0042]
[Effect of the Invention] As explained above, a user is enabled to perform the check and processing of updating automatically only within his user information, and the time and effort of management of the user information on an authentication system is mitigated by this invention by this. Moreover, according to the registration situation of a public key certification certificate, it becomes possible to perform registration and deletion of user information. Therefore, an authentication system side can offer check service and updating service of user information, and it becomes possible to relate registration processing and deletion of user information with management of a public key certification certificate, and to perform them certainly.

[Translation done.]

Drawing selection | Representative drawing



[Translation done.]

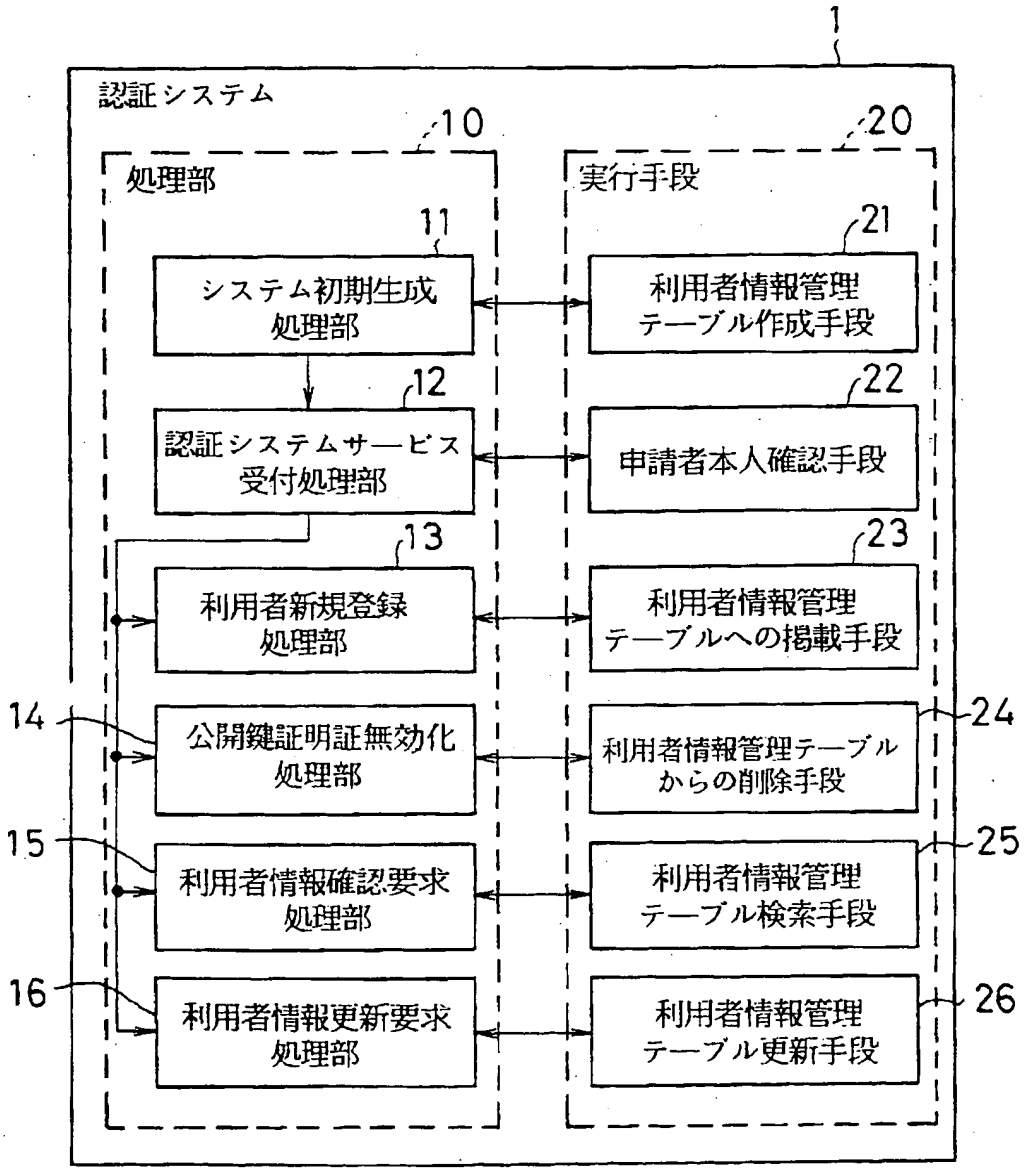
DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is the block diagram showing the configuration of the authentication system concerning this invention.
[Drawing 2] It is a block diagram for explaining the initial generation processing of a system in drawing 1 .
[Drawing 3] It is a block diagram for explaining the authentication system service reception processing in drawing 1 .
[Drawing 4] It is a block diagram for explaining the user new registration processing in drawing 1 .
[Drawing 5] It is a block diagram for explaining the public key certification certificate nullification processing in drawing 1 .
[Drawing 6] It is a block diagram for explaining the user information acknowledge request processing in drawing 1 .
[Drawing 7] It is a block diagram for explaining the renewal demand processing of user information in drawing 1 .
[Description of Notations]
11 Initial Generation Processing Section of System
12 Authentication System Service Reception Processing Section
13 User New Registration Processing Section
14 Public Key Certification Certificate Nullification Processing Section
15 User Information Acknowledge Request Processing Section
16 Renewal Demand Processing Section of User Information
21 User Information Management Table Creation Means
22 Applicant -- Principal Check Means
23 Printing Means to User Information Management Table
24 Deletion Means from User Information Management Table
25 User Information Management Table Retrieval Means
26 Renewal Means of User Information Management Table
21a User information management table
22a Application
22b Public key certification certificate management database

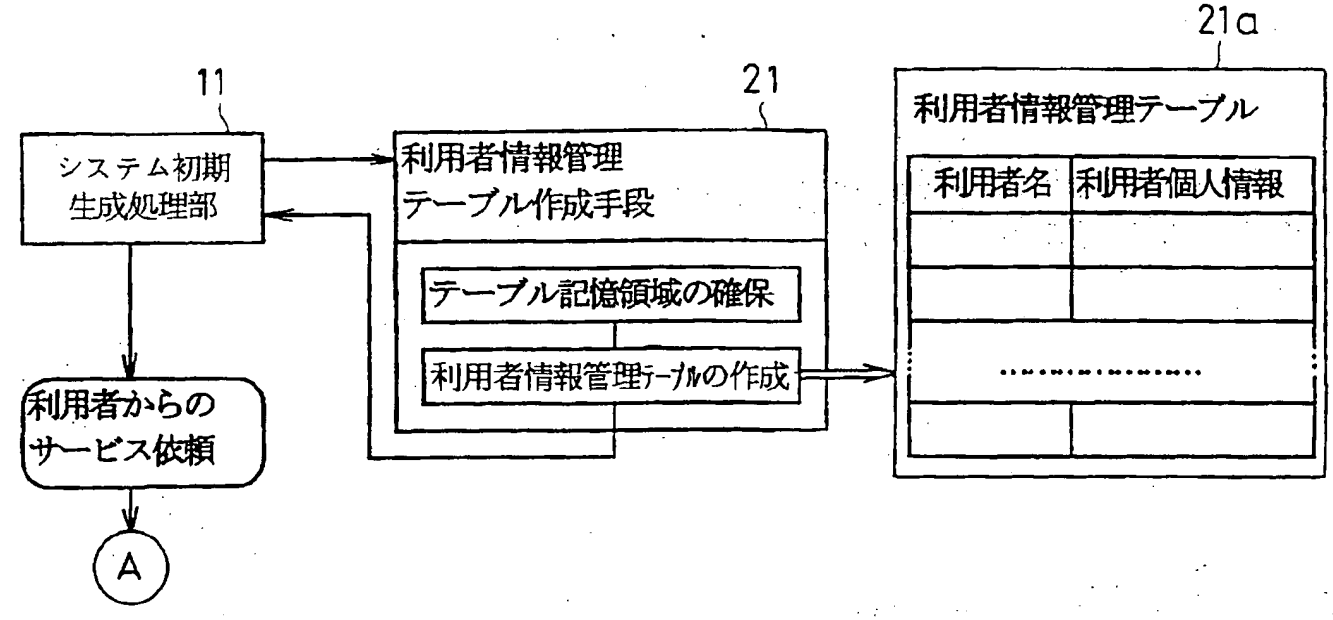
[Translation done.]

DRAWINGS

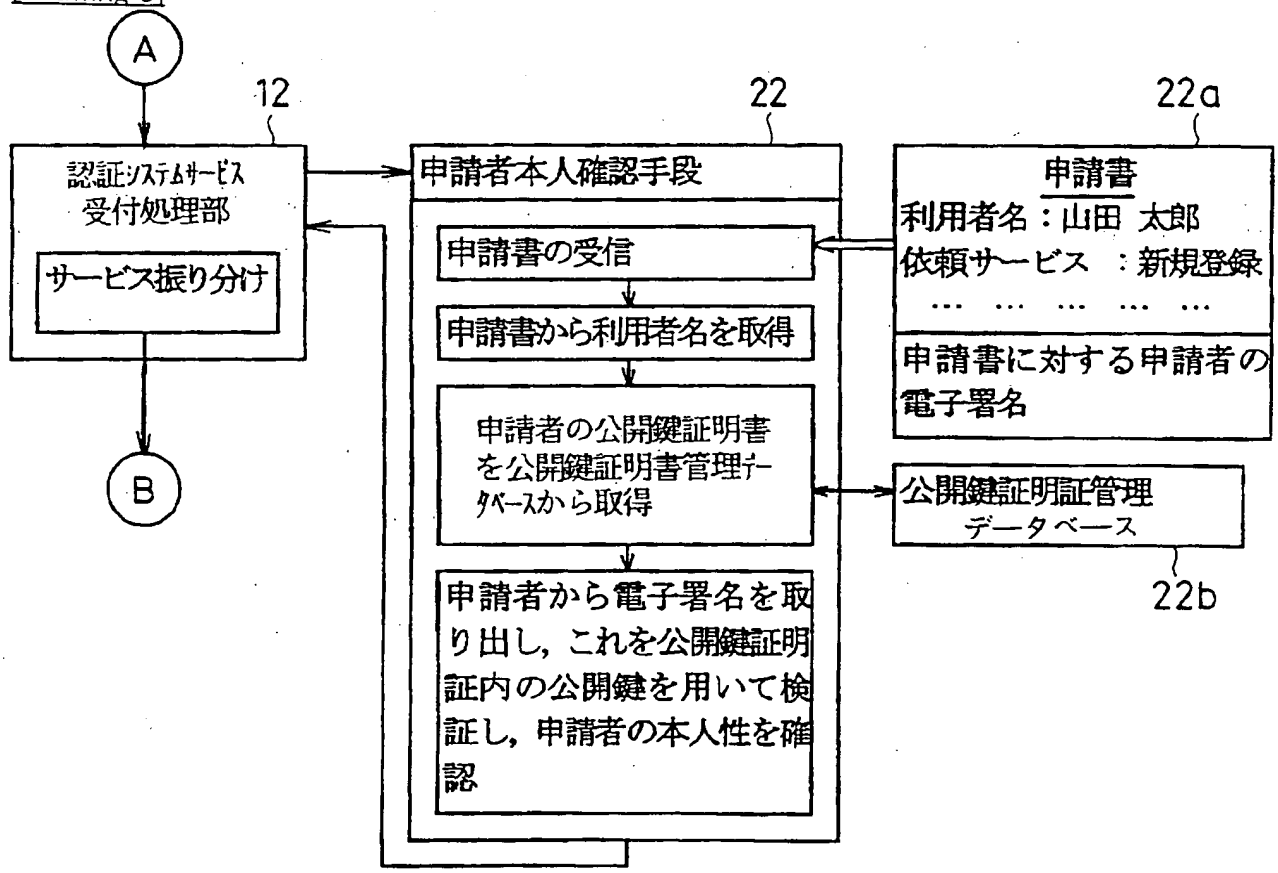
[Drawing 1]



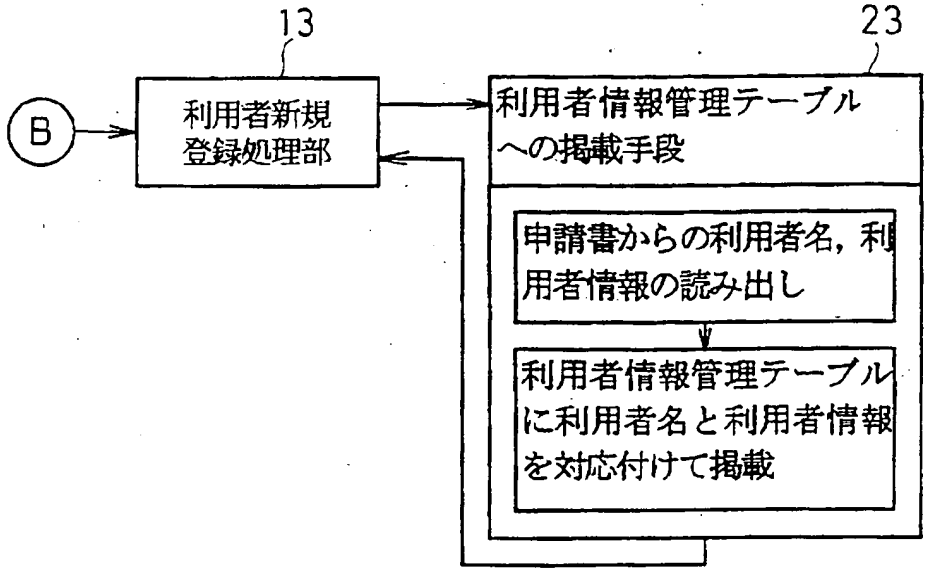
[Drawing 2]



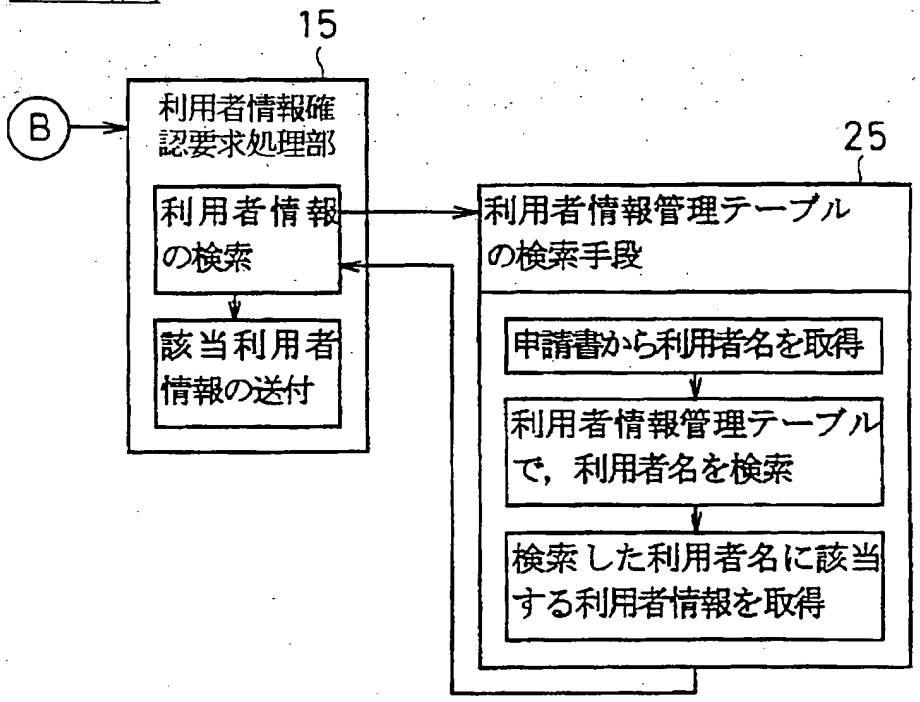
[Drawing 3]



[Drawing 4]

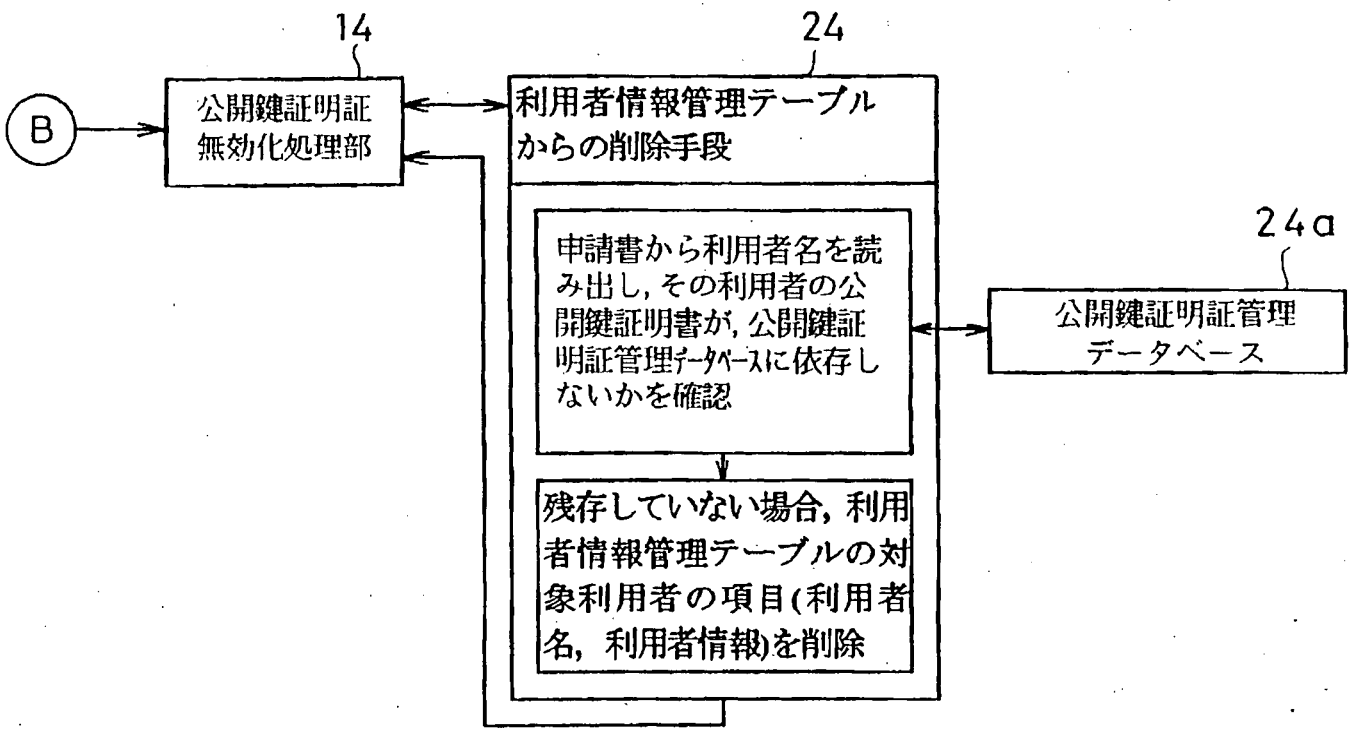


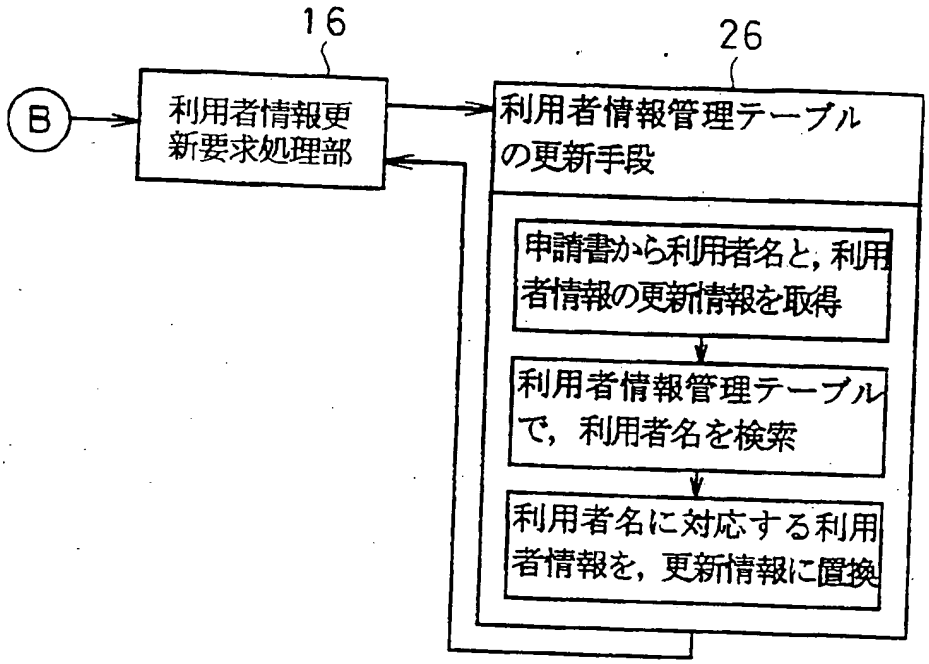
[Drawing 6]



[Drawing 5]

[Drawing 7]


14
24
B
公開鍵証明証
無効化処理部
利用者情報管理テーブル
からの削除手段
申請書から利用者名を読み出し，その利用者の公開鍵証明書が，公開鍵証明証管理ﾃﾞｰﾀﾍﾞｰｽに依存しないかを確認
残存していない場合，利用者情報管理テーブルの対象利用者の項目(利用者名，利用者情報)を削除
24a
公開鍵証明証管理
データベース



[Translation done.]

Japanese Patent Application Public-disclosure No. 10-285156
Japanese Patent Application Public-disclosure date: October 23, 1998
Title of the invention: User information management device in an authentication system
Japanese Patent Application No. 9-92436
Japanese Patent Application date: April 10, 1997

~ omitted ~

[0025]

On the contrary, when the authentication system receives a request from an applicant to provide public key certificate revocation service, the operation proceeds to step S4, where, at the public key certificate revocation processing section 14, it is first confirmed, by using the cancellation means 24 from the user information management table 21a, that the applicant's public key certificate does not remain in the public key certificate management database 24a, and upon confirmation, items (user name, user information) pertaining to the user are deleted from the user information management table 21a.

~ omitted ~

[0032]

Next, referring to Fig. 5, public key certificate revocation processing performed at the public key certificate revocation processing section 14 will be specifically described. If a requested service entered in the application form 22a submitted by a user is public key certificate revocation service, processing is transferred to the public key certificate revocation processing section 14 by means of service dividing processing. The public key certificate revocation processing section 14 registers, in a revocation list, the public key certificate that the user asked to revoke and deletes the public key certificate from the public key certificate management database 24a. At this time, the deleting means 24 for deleting information from the user information management table 21a is invoked.

[0033]

The deleting means 24 for deleting information from the user information management table 21a first reads a user name from the application form 22a and confirms that the user's public key certificate no longer remains in the public key certificate management database 24a managed by the authentication system. If it is confirmed that the user's public key certificate does not remain in the authentication system, it is no longer necessary for the authentication system to manage the user's user

information and thus, the items (user name and user information) relating to the user are deleted from the user information management table 21a. Thereby, it becomes possible to efficiently utilize a management domain for the user information.

[0034]

The public key certificate database 22b can be easily searched by any common authentication system.

Fig. 1

Authentication system

Processing section

11: system initial production processing section

12: authentication system service acceptance processing section

13: user new registration processing section

14: public key certificate revocation processing section

15: user information confirmation request processing section

16: user information update request processing section

Execution means

21: user information management table generation means

22: applicant identification means

23: means for inserting information into a user information management table

24: means for deleting information from a user information management table

25: user information management table searching means

26: user information management table updating means

Fig. 3

12: authentication system service acceptance processing means

(dividing service)

22: applicant identification means

(acceptance of an application form)

(obtaining a user name from the application form)

(obtaining the applicant's public key certificate from the public key certificate management database)

(retrieving an electronic signature from the application form, verifying the signature by means of a public key in the public key certificate and determining the identification of the applicant)

22a: application form

user name: Taro Yamada

requested service: new registration

Electronic signature of an applicant who submitted the application form

Public key certificate management database

Fig. 5

14: public key certificate revocation processing section

24: means for deleting information from the user information management table

(reading a user name from the application form and checking if the user's public key certificate remains in the public key certificate management database)

(if it transpires that it does not remain in the database, items concerning the user are deleted from the user information management table)

24a: public key certificate management database